9.3 Scanning
DEMO Scanning a Target Network DEMO

- In this process are refers to a set of procedures identifying a network or a target machine, ports, and services is probed by the attacker to exploit the vulnerabilities. Some of the tools used in this process are Nessus, Nexpose, Nikto and NMAP etc.
- Network scanning is performed to check for live systems, open ports, banner grabbing or OS fingerprinting and vulnerabilities and to draw network diagrams of vulnerable hosts.
- DEMO
- Lab Analysis

9.3 Scanning
DEMO Scanning a Target Network DEMO

- Nikto is a open source scanner on Linux , Windows etc.

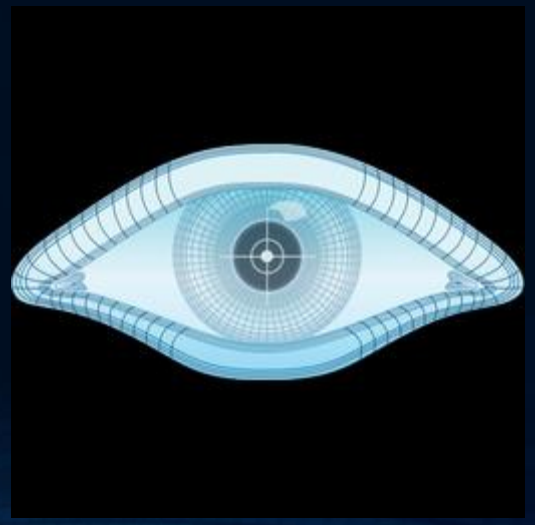
`Nikto -help`

`nikto -h thewebchecker.com` (simple scan)

`nikto -host` www.hackthissite.org `-Tuning 1` (1 – Interesting File / Seen in logs)

9.3.1 Scanning System and Network Resources using Advanced IP Scanner DEMO

- Advanced IP Scanner or **Zenmap** Linux is a free network scanner that gives you various types of information regarding local network computers.
- DEMO
- Lab Analysis



9.3.4 Wireshark DEMO

- **Wireshark** is the world's foremost and widely-used network protocol analyzer. It lets you see what's happening on your network at a microscopic level.

9.4 Gaining Access (Enumeration) Enumerating a Target Network

- In this process, to enter into the system, vulnerabilities are located and attempts are made to exploit. The main tool used in this process is Metasploit. Is about extracting user names, machine names, network resources, shares and services from a system.

9.4.1 Enumerating NetBIOS using the SuperScan tool DEMO

- **SuperScan** is a TCP port scanner, Pinger and resolver.
- DEMO
- Lab Analysis